# 2020 CTPRA Certification Job Practice Guide

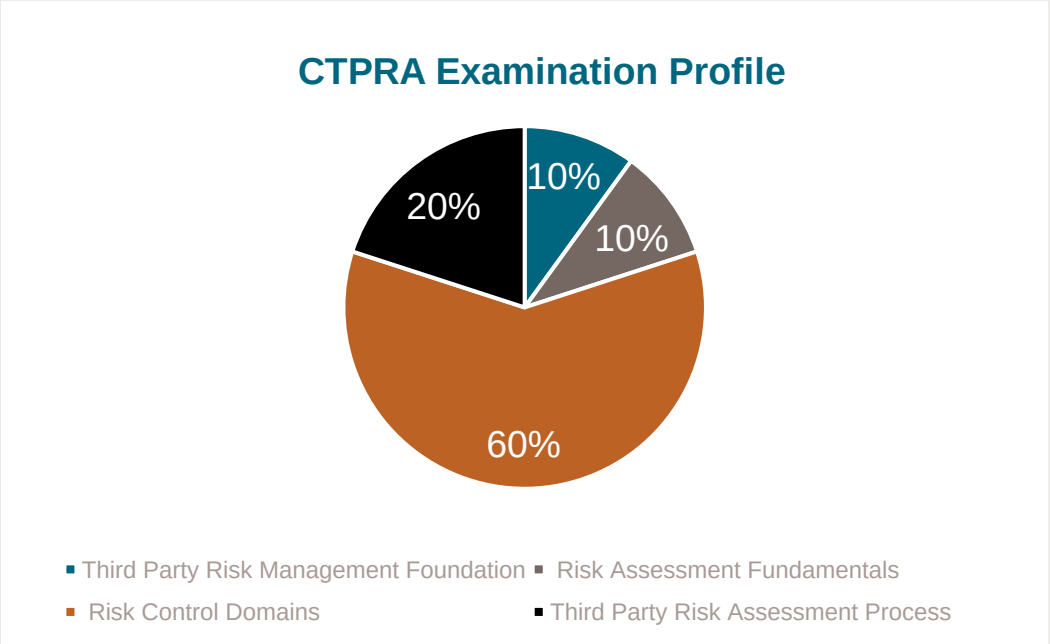
## *Role Description*

The CTPRA designation is designed to validate knowledge and experience within specific third-party risk management competencies that an individual will need to be able to conduct a thorough risk evaluation of a third party during an assessment including risk analysis and reporting. The job practice guide identifies the domains, topics, skills, competencies, and job role accountabilities that represent the type of work performed in the role of a third-party risk assessor who plans, performs, and oversees third party assessments across multiple risk domains. The structure of the job practice guide is based on the inputs of Shared Assessments Program members, recognized best practices, education and tools that drive third party risk assurance.

## *Certification Blueprint*

To achieve the CTPRA credential, candidates must provide both evidence of their years of experience and successfully passing a rigorous exam. It is not uncommon for CTPRA test takers to not pass the test on the first attempt. Earning a qualified credential, requires prior knowledge and simply completing a training course does not guarantee you will pass the test. We recommend at least **30** hours of preparation prior to taking the examination. The course materials and examination are career resources designed for those professionals who plan to certify, as well as for those who simply need to deepen their knowledge in third party risk management.

The CTPRA training material and examination is organized by grouping the required body of knowledge topics into specific job practice focus areas. The CTPRA examination will contain questions testing domain technical knowledge and application of on-the-job knowledge based on the CTPRA Curriculum Outline:




## *Examination Protocols & Question Formats*

The CTPRA examination will contain 125 questions worth up to 140 points. Examination questions will include testing the domain technical knowledge and application of knowledge using third party risk situations.

The CTPRPA examination is a time-based, closed book exam, completed within 2 hours. The exam is taken online, and remote proctoring will be required to monitor examination compliance. Upon completion of the exam a survey may be presented to provide feedback on the method of instruction, curriculum, materials, or examination content.

Multiple choice questions will be presented to users using third party risk management scenarios from the outsourcer or the service provider point of view.

### Example#1:

### Knowledge Based Question

Perimeter controls are part of the first layer of defense to prevent unauthorized physical access, as well as accidental and intentional damage to the organization's physical premises, systems, and information. Which of the following is NOT considered a perimeter control:

A. Building monitoring and intrusion alarms
B. Personnel Access Controls
C. Firewall Logs
D. Environmental controls

## Example#2:

### Controls Evaluation Focus Question

When conducting a perimeter security review, the most effective sequence of testing the physical security controls is:

A. Test restricted entry areas first
B. Test public areas of the building first
C. Test only the exterior areas of the building
D. Start on the outside of the building and work inward

## Example#3:

### Multiple Choice/Factors Question

Physical access logs should:

A. Be kept for no more than 60 days

B. Record both successful and unsuccessful access attempts

C. Include the investigation of unsuccessful access attempts

D. Apply only to server rooms or data centers

**Select which set of choices represents the best selection**

- A, B, C
- B, C
- A, D
- A, B, C, D

## Example#4:

### Scenario-Based Question

A. You are a third party risk analyst, conducting a review of your TPRM program. When quantifying the actual resource requirements to operate your program which metric is least important in assessing whether your current resources can achieve your program goals? The number of people you need to perform control assessments based on your policies
B. The dollar amount of your budget
C. The number of people you need to maintain the program

The number of people you need to interpret vendor responses

*Body of Knowledge*

## I. Third Party Risk Management Foundation

A. Regulatory Drivers for Third Party Risk
B. Information Classification and Data Governance
C. Third Party Risk Management Program Components

## II. Risk Assessment Fundamentals

A. Assessment Frameworks and Standards
B. Risk Assessment Techniques
C. Vendor Classification and Due Diligence Requirements

Types of Third-Party Risk Assessments

## III. Risk Control Domains

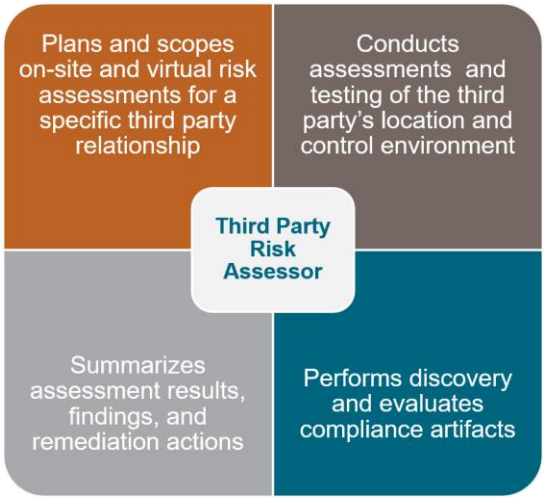
A. Governance & Risk Management
    1. Risk assessment & treatment
    2. Information security policy
    3. Organizational security
    4. Data Privacy Governance
    5. Human resources security
    6. Compliance & Audit
B. Information Protection
    1. Access control
    2. End user device security
    3. Server security
    4. Network security
    5. Application security
    6. Data Privacy Safeguards/Information Systems
    7. Cloud security
    8. Physical & environmental security

C. IT Operations & Business Resiliency
    1. Asset management
    2. Operations management
    3. Business Continuity Management
    4. Disaster Recovery
D. Security Incident & Threat Management
    1. Incident event and communications
    2. Threat management
    3. Vulnerability program
    4. Security awareness

**IV. Third Party Risk Assessment Process**

A. Phases of an Assessment
B. Assessment Planning and Preparation Activities
C. Assessment Execution and Communication
D. Post Assessment Reporting & Remediation

*Role Accountabilities*




- Actively drives coordination and execution of conducting third party risk assessment reviews either on-site or through virtual assessments.
- Participates in the creation, development, deployment of security and risk plans and mitigation controls
- Manages and deploys third party risk intake, assessment, remediation, risk acceptance and communication processes
- Conducts security, vulnerability and control assessments using standard methodologies
- Plans and coordinates testing and verification of controls
- Reviews compliance artifacts and technical materials to identify and evaluate controls
- Monitors existing and proposed security, risk, and control frameworks
- Monitors changes in regulation that impact third party risk
- Builds and manages remediation plans for third party due diligence risk assessments
- Manages and maintains information in governance, risk, compliance systems and tools
- Prepares reports on risk ratings, findings, and assessment results.
- Identifies and evaluates compensating controls based on risk mitigation techniques
- Analyzes complex situations where an in-depth evaluation of risk is required
- Accountable to synthesize information to technical and non-technical audiences
- Ability to use judgement within established policies and procedures to evaluate control effectiveness and control attributes
- Creates management reporting on third party risk activities across multiple engagements
- Conducts audits or assessments in alignment with standards and risk based strategies
- Conducts interviews with subject matter experts to gain thorough understanding of the control environment.
- Identifies synergies and dependencies in planning third party assessments

- Manages project management timelines, status reports, findings, results, and recommendations to stakeholders.
- Interacts directly with key personnel within both IT and lines of business to understand the roles and responsibilities